International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-7, Issue-2, March 2019
DOI: 10.21276/ijircst.2019.7.2.1

Multi-Layered Security System Using Cryptography and Steganography

Mahima N, Noor Siddiqa, Tanvir Habib Sardar

***Abstract*—The Internet as a whole does not use secure links, thus information being transmitted may be vulnerable to interception as well. The importance of reducing the chances of information being detected during transmission is a major issue. A solution to be discussed is how passing of information can be done in a manner that the very existence of the message is unknown. This is important in order to repel attention from the potential attacker. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection of digital media. In this work, we focus on the achievement of a multi-layered security system by combining both cryptography and steganography. Encryption avoids passive attacks (reading) and by steganography, the message becomes undetectable. We make use of AES algorithm and Least Significant Bit (LSB) technique for hiding messages in an image. We have enhanced the LSB technique by randomly dispersing the bits of the message in the image and thus making it harder for an unauthorized person to extract the original message. The AES provides a good security as it takes considerably much more time to break by the brute force method for a given key length. The proposed methodology is proved good and produced expected output.**

***Index Terms*—Information Security; Cryptography; Steganography**

I. INTRODUCTION

Intruders are successful in many cases in retrieving information because that most of the information they acquire from a source is in a form that they can read and comprehend. These attackers may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack.

Manuscript Received March 19, 2019

Mahima N, Dept. of Cloud Technology and Information Security, School of Engineering and Technology, Jain University, Bengaluru Country Name, Mobile No: 9731683341, (e-mail: mahimamahigowda@gmail.com)

Noor Siddiqa, Dept. of Cloud Technology and Information Security, School of Engineering and Technology, Jain University, Bengaluru Country Name, Mobile No: 9663926580

Tanvir Habib Sardar, Assistant Professor, School of Engineering and Technology, Jain University, Bengaluru Country Name, Mobile No: 8147669016

This problem of Unwanted information retrieval can be solved by using cryptography or steganography.In data and telecommunications, Cryptography is used as a mechanism to protect data and provide secure communication over an unsecured network such as the internet. It can also be used to provide an additional security mechanism to protect passwords in the database to prevent them from being human readable or understandable [1]. It is important to note that cryptography is necessary for secure communications, but it is not itself sufficient [2]. An encrypted message may draw suspicion while a hidden message will not. This motivated us to develop a multilayered security system by combining cryptography and Steganography to enhance the security of the data to be stored and send. Steganography is the art of concealing the existence of information within seemingly innocuous carriers. The purpose of steganography is to send secret messages by hiding data into some innocuous cover-objects such as digital images and to reduce the possibility of being detected by any third party. The advantage of steganography over cryptography is that, in steganography messages do not attract attention to themselves. Plainly visible encrypted message will arouse suspicion, no matter how unbreakable or strong the method used for encryption is .Cryptography protects the contents of a message but steganography protects both the message as well as the communicating parties [3].

Steganography can be used to maintain the confidentiality of valuable information and to protect the data from possible sabotage, theft, or unauthorized viewing [4]. The purpose of this work is to develop a multilayered secure system for storage and transferring the information over an unsecured network. This is achieved by combining cryptography and steganography techniques. The goal of this work is to secure data for storage and transfer over an unsecured network.

The rest of the paper is organized as follows. The proposed system of work i.e. methodology is explained in section II. Section III provides results. The last two sections conclude our work and provide future work.

II. METHODOLOGY

This section describes the overall view of a proposed system and its sub system. The different sub-systems give their unique functionality which when put together provides an effective, user-friendly and reliable system which fulfills the objectives. The system provides an overview of the system. The key components are:

- Login- The system establishes the identity of the user and makes available the list of actions.

- Data securing and retrieval- user can secure data by encrypting it and hiding it inside an image. User can also get back the data by desteganography and decryption.
- Logout- once the user finishes the process he can logout.

A user registration page is used where a new username and password should be entered. A database Management which manages the contents of the page where the user data details are stored. Data encryption process using AES algorithm and data decryption is also added. Image steganography is done by LSB insertion. The image is attached to a mail and sent to the recipient.

Data securing job is performed by the login operation with a valid user name and password, selects a text, image or file to be encrypted, selects the carrier image and enters a password which is used as a key for encryption.First compression is performed on data then encryption is done on data after that steganography is performed. The result is an image in which the data is hidden. The image is send as an email to particular user select by sender.

Data retrieval process is started when the user selects the appropriate image to be destegnographed; the user receives the steg-images from the web server through their respective emails. After selecting image user should enter the valid key or password and clicks on the decrypt button. The hidden message, file or image is thus retrieved. Key is assumed to be transferred between the sender and receiver in secured way. The division of system is done according to the separate functionalities that our system provides. Based on the functionality, we have divided the entire system into four modules.

1. Encryption decryption module
2. Steganography module
3. Compression module
4. User interface module

The first three modules are responsible for the multi-layered security of the system.The AES algorithm [5][6] is made use of in the first module for encryption and decryption. It is a fast, strong and superior to algorithm like DES. AES algorithm makes use of a cipher key which can be 128, 192 or 256 bytes in size. The input keys should be of 128 bytes. The second module makes use of the LSB insertion technique. This method is implemented by replacing the LSB's of redundant bytes of an image with the bits of the binary form of the encrypted message. The original image on whose bits are replaced is called the carrier image. The final image is called the stego image.The third module is compression which reduce the size of data to be hidden before doing encryption, the major advantage of using compression is more data can be transferred and it provides one more layer of security, since compressed will be not be in readable format.In the final module, functionality is provided such that the user authentication, registration account block, selects a carrier image and enters the secret message. The carrier image and the secret message then undergo encryption and steganography. The final image is then sent to the authenticated receiver. The receiver has to enter a personalized key in order to view the message.The sequence of steps carried out in this system is depicted by the flow chart shown in figure 1 and 2.

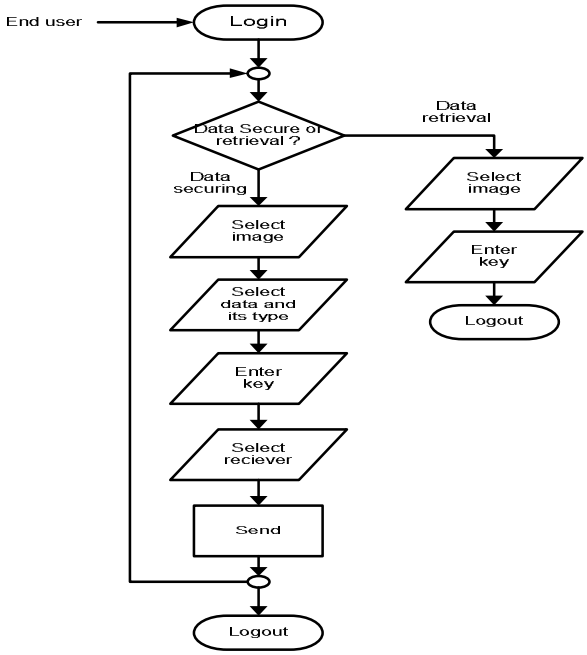

Fig.1: Functional Descriptions of the Modules

The implementation begins with an authentic user logging in. The user has to select an option to perform the data securing or retrieval operation. If the user selects the encryption option, he is given a choice between a secret image, secret file or a secret text i.e. the user can choose to select a text, a file or an image to be hidden in the cover image. Encryption is carried out after the user has entered a password or key. The resulting image is mailed to the receiver. Decryption requires the user to enter a password in order to extract the hidden message from the cover image. On completion of a transaction, the users can logout.Encryption module: we implement AES algorithm for encrypting the secret data.

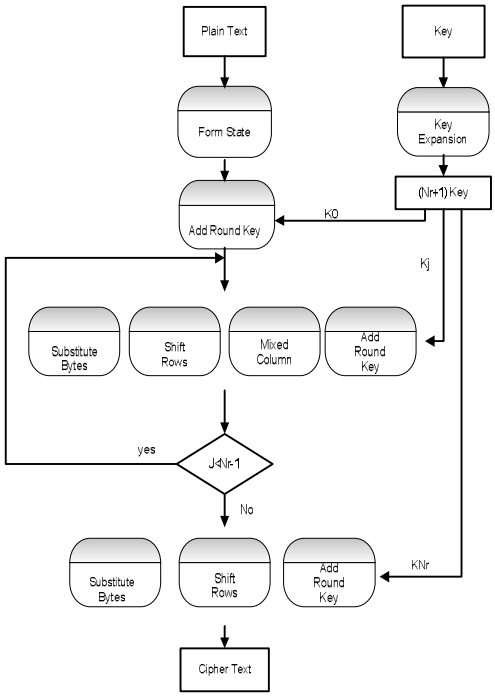

Fig.2: Cryptography process using AES algorithm

Steganography[7][8]: Least significant bits (LSB) insertion is a simple approach to embedding information in image file. The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small. The encrypted secret message is converted into an 8-bit binary representation. The cover image also called the carrier image is also converted into its 8-bit representation. The secret message is then broken down to its individual bits by a steganographic tool (stego-tool) and hidden in the cover object. We hide 1 bit of the embedded message for every 8 bits of the cover image. Many tools will utilize a password or passphrase which is necessary to extract the hidden message and is referred to as a stego-key. The result of this process is known as the stego-object.The reverse process is called de-steganography. Here, the steg-image which is downloaded by the receiver from the mail is converted to its 8-bit representation. This conversion makes it easier to undergo the process. The resulting 8-bit representation can eventually be split into the carrier image and the secret message which is obtained by combining LSBs Fig 8 shows the steps involved in destegnography and to retrieve the data.

III. TEST CASES AND RESULT

In this section we have provided different test cases which provide a basis for result we obtained.

Unit Test cases:In this section we discuss the various unit test cases for encryption, decryption, steganography, compression and so on and their effects on various inputs.

Test cases for encryption: First we will go for the test for the encryption of text. The selected text is given as Input and we are getting then encrypted text. So the encryption unit works as intended. Next test for the encryption of the image and file. Give the image and file as input for the test separately as we are getting the encrypted image of the image and File the encryption unit works as intended.

Test cases for steganography: The following mentioned test cases are executed. They determine whether steganography is done. Here,data and carrier image are given as Input. After test we are getting steganographeddata .The data is hidden in the image. The steganography unit works as intended.

Test cases for decryption: A careful analysis is carried out to check if it gives an expected output. Data to be decrypted which is in the form of image is given as the input. We are getting the actual image as Output. So the decryption unit works as intended. Next we are giving the data and file to be decrypted which is in the form of text and file respectively. And we are getting the original text and original file as the actual output.

Test cases for desteganography: Steg-image i.e. image in which data is hidden is given as the input. Desteganography text cases have to be executed to obtain output getting original data as actual output which is the expected one. The data is extracted. The desteganography unit works as intended.

Test cases for compression: Then test cases are run to test the compression module.Give the data to be compressed and the expected outcome is compressed data.AfterTesting the outcome is compressed data.After careful analysis, it is observed that the above test cases give expected results for favorable outputs and thus, the units are fit for encryption.

Integration Testing
Integration test checks module compatibility, system and acceptance tests check behavior of the whole system with respect to specifications and user needs respectively.

Integration Test case1: The following section describes the test cases where two or more unit test cases are combined and analyzed. Here, we observe the effects of different integrated modules on different inputs.

Integration test case 1 is to validate whether the data can be encrypted and then decrypted. Data is given in the form of image, file or text. The data is successfully encrypted and then decrypted to get the original data.

Integration test case 2 is to validate whether the data can be compressed and then encrypted.Input is the Data to be encrypted and the output is successfully compressed and encrypted data.

Integration test case 3 is to validate whether the data can be hidden in the image. Data to be hidden and carrier image are given as input. After the test we can observe that the data is successfully encrypted and hidden inside the image.

Integration test case 4 is to validate whether the data can be extracted and decrypted and the input given is carrier image. as output we have successfully extracted and decrypted data.

Integration test case 5 is to validate whether the compressed data is encrypted and steganographed. Here also carrier image is given as the input and after the test we are getting the successfully compressed, encrypted and hidden inside the image

Integration test case 6 is to validate whether the data can be desteganographed, and decrypted.Input is carrier image, and key for decryption.After the test we can see that the data is extracted, decrypted and decompressed It can thus be concluded that the above integration test cases give expected results for favorable outputs

System Testing
The whole system has been tested for functionality through relevant test cases. The test has been also done to check whether the data is properly stored or not. All links have also been tested for functionality.

User interface Test Cases: The following test cases depict the different user interface system test cases. It analyses whether favorable outputs are obtained for different user actions

System test case 1 is to validate whether the username and password combination is valid. Input is Username and password in the login page. And the expected output is the Redirection to the encryption page and the user is getting a successful login.

System test case 2 is to validate whether the registered new user has entered valid details. Input is new user name and password and here the control is transferred to the login

page .And the output is Dialog box saying new user registered. The user can now login and use the system as an existing user.

System test case 3 is to validate whether the username and password combination is valid. Username and password in the login page are the Input. Here it is redirected to encryption page and we got expected Invalid login error message

System test case 4 is to validate whether the carrier image and key combination is valid. Input is Carrier image and the expected outcome is successful decryption and desteganography. As result we are getting Invalid password error message. The data is not decrypted and desteganographed. The user has entered the incorrect key for the corresponding carrier image.

System test case 5 is to validate whether the registered new user has entered valid details. As we are giving new user name and password as input user name re-entry request is displayed. That is the user name and password already exists in the database. The user will have to enter a unique username and password combination.

System test case 6 is for Account blocking during login. Input is Username and password. Expected output is after the third incorrect entry of username and password combinations, the corresponding username should be blocked and we are getting it.

System Test Cases

The following test case provides an analysis of the system as a whole. It gives a description of whether an expected result is obtained for a specific output. This test case is a combination of integration test cases.

Table 1: System test case 1

Test case No.	STC 1
Description	To validate whether the carrier image and key combination is valid.
Input	Carrier image, data to be hidden, receiver name and key.
Expected Output	Successful data securing and the system mails the resulting image to the recipient.
Actual Output	Successful data securing and the system mails the resulting image to the recipient.
Result and Remarks	The data is successfully secured. The user has entered the correct key for the corresponding carrier image.

Table 2: System test case 2

Test case No.	STC 2
Description	To validate whether the carrier image and key combination is valid.
Input	Carrier image and key.
Expected Output	Successful data retrieval and the receiver will get the hidden data.
Actual Output	Successful data retrieval and the receiver will get the hidden data.
Result and Remarks	The data is successfully decrypted and desteganographed. The user has entered the correct key for the corresponding carrier image.

IV. CONCLUSION

This work achieves all the objectives listed. It is successful in achieving a multilayered secure system which combines the security features of cryptography and steganography. Steganography can be used for hidden communication. We have explored the limits of steganography theory and practice. We pointed out the enhancement of the image steganographic system using LSB approach to provide a means of secure communication. A stego-key has been applied to the system during embedment of the message into the cover-image. Finally, we have shown that steganography that uses a key has a better security than non-key steganography. This is so because without the knowledge of the valid key, it is difficult for a third party or malicious people to recover the embedded message. However there are still some issues need to be tackled to implement LSB on a digital image as a cover-object using random pixels. Steganography is not intended to replace cryptography but rather to supplement it. If a message is encrypted and hidden with a steganographic method, it provides an additional layer of protection and reduces the chance of the hidden message being detected

V. FUTURE WORK

Changes to software are a must. Changes could be to improve the performance of the system in terms of user-friendliness, additional features etc.In this paper, we have only dealt with encryption and steganography of images, text and document, text or pdf files. However, this can also be implemented on audio or video files. To do this, the carrier object needs to be an audio or video file depending upon the encrypted data.Apart from the steganographic and cryptographic improvements, features can also be added to the user interface. We have assumed the exchange of the encryption key. A feature to actually exchange the key between sender and receiver can also be added.

REFERENCES

[1]An Overview Of Crptography-9 November 2010,By Gary C Kessler

[2]http://www.garykessler.net/library/crypto.html#intro

[3]Improving Embedding Efficiency Of Covering Codes For Applications In Steganography By WeimingZhang,ShuozhongWang,AndXinpeng Zhan

[4] A detailed look at Steganographic Techniques and their use in an Open Systems Environment- By Bret Dunba.

[5].Implementation and Analysis of AES, DES and Triple DES on GSM Network, MajithiaSachin Lecturer, Department of Information Technology, Chandigarh Engineering College Landran (Mohali, PB), India, 2010

[6].AES Advanced Encryption Standard CSC 7002 Computer Security by William Roche, University of Colorado, Denver, May 2006

[7] NavitaAgarwal, Himanshu Sharma "An Efficient Pixel-shuffling Based Approach to Simultaneously Perform Image Compression, Encryption and Steganography", IJCSMC, vol. 2 issue 5, pp. 376-385, May 2013.

[8] Gary C.Kessler, "An Overview of Cryptography: Cryptographic", HLAN, ver. 1, 1999-2014

